REMARKS

Claims 1-27, 41-59, 71 and 72 are pending in this application. After claim amendments herein, claims 1-27, 41-59, 71 and 72 will remain pending in this application.

In the March 6, 2006 final Office Action, the Examiner rejected claims 1-27, 41-59, 71 and 72 under 35 U.S.C. §103(a) as being obvious based upon U.S. Patent Application Publication No. 2003/0196098 (Dickinson) in view of U.S. Patent Application Publication No. 2004/0168079 (Motoyama). Applicants traverse this rejection.

The undersigned attorney for Applicants first thanks the Examiner for the courtesies extended during telephone conferences on September 19 and 22, during which the prior art and the claims on file were discussed and during which the undersigned attorney suggested distinctions between the prior art and the present invention and suggested amendments for overcoming the Examiner's rejections. The arguments and amendments discussed have been presented herein for full consideration by the Examiner.

Dickinson relates to an e-mail firewall that applies policies to e-mail messages between a first site and a plurality of second sites in accordance with administrator selectable policies. The firewall comprises a simple mail transfer protocol (SMTP) relay causing the e-mail messages to be transmitted between the first site and the second sites, and a plurality of policy managers enforce-administrator selectable policies. The policies comprise at least a first source/destination policy, at least a first content policy and at least a first virus policy, and are characterized by a plurality of administrator selectable criteria, a plurality of administrator selectable exceptions to the criteria and a plurality of administrator selectable actions associated with the criteria and exceptions. The policy managers comprise an access manager, a content manager and a virus manager for restricting transmission of e-mail messages between the first site and the second sites in accordance with the source/destination policy, the content policy and the virus policy, respectively.

It is clear that Dickinson teaches a system that deals only with messages that are incoming into the first site, in accordance with a series of policies. At paragraphs [0022-0029], Dickinson discusses the manner in which messages received from internal and external sites are processed by a policy engine and a plurality of policy managers, which comprise modules for enforcing policies directed to specific aspects of e-mail messages, such as source/destination access policies, content control policies, virus control policies and encryption/decryption policies, that have been selected by the e-mail firewall administrator. The policy engine, using the policy managers to enforce the pre-selected policies, determines which policies are applicable to a message by building a list of policies for the sender (source) of the message and building a list policies for each recipient. The policy engine calls the policy managers to apply each policy, based upon their order of priority, and then receives results from policy managers and transmits messages to the SMTP relay module in accordance with the received results. The results received by the policy engine comprise actions such as disposition, annotation, and notification, and the result of processing of a message by the policy engine can result in generation of a plurality of additional messages, for example, for notification to the sender or recipient, or to the system administrator.

Paragraphs [0030-0031] of Dickinson refer to one embodiment wherein security usage policies specify that certain users, under certain conditions, should perform encryption and/or signature at the desktop. The example used in paragraph [0030] is an e-mail from a company's CEO to the company's legal counsel that can be specified to require either encryption and/or signature in order to enforce attorney-client privilege and to preserve encryption policies. Moreover, client security usage policies can be used to specify that messages, which are already in encrypted form and perhaps meet some other criteria, should be preserved and not be processed, modified or encrypted by the e-mail firewall. Paragraph [0031] specifies that policies are entered preferably by an authorized administrator by way of a configuration module in the form of a program executing on a stored program computer and can be applied to users, either individually or by e-mail domains or other groupings.

Applicants point out to the Examiner that, as opposed to the Dickinson system, wherein the firewall policies control the disposition of the incoming message, the present invention relates to a system wherein the communication itself controls its disposition wherever the communication may be sent. In order to clarify this and to more distinctly claim the subject matter of the invention, Applicants have amended claim 1 to recite a system comprising a first memory containing a program executable by a processor to attach a privileged attribute to a digital communication and create a privileged distribution list of at least one intended recipient and associate the privileged distribution list with the digital communication. Amended claim 1 also now recites a second memory containing a program executable by a processor to restrict access to and routing of the privileged digital communication to the at least one intended recipient according to the privileged distribution list associated with the digital communication, as well as store the privileged digital communication in a segregated location for privileged digital communications on a data storage device. Claim 71 has been similarly amended to recite a digital communication system having a first memory containing a program executable by a processor to attach a privileged attribute to a digital communication and a second memory containing a program executable by a processor to restrict access to the digital communication in accordance with the privileged attribute attached to the communication.

By contrast, while it is true that the attachment of files, including executable files, to e-mail messages is a known feature, as set forth in Motoyama, neither Dickinson nor Motoyama teaches a first memory containing a program that is executable to attach a privileged attribute to a digital communication (claims 1 and 71) and create a privileged distribution list and associate it with the digital communication (claim 1) and a second memory containing a program that is executable to restrict access to the digital communication in accordance with the privileged distribution list (claim 1) or the attached privileged attribute (claim 71).

Similarly, claims 18 and 72 have been amended to clarify that the digital communication system comprises a memory containing a program executable by the processor attach an executable module to a digital communication, which module restricts access to and routing of the digital communication to which it is attached. Claims 49 and 57 have been amended to clarify that the method for creating a digital communication or document comprises the steps of creating an executable module for instructing a computer to restrict access to the attached communication/ document according to an associated privileged distribution list and attaching the executable module to the communication, whereby the module instructs the computer to restrict access to the communication/document according to the associated privileged distribution list.

In amended claims 18, 49, 57 and 72, the steps of restricting access to and routing of the privileged communication to the privileged distribution list are taken under instruction from an executable module that is attached, by a program stored within a memory and executable by a processor, to the very digital communication to which it is attached. By contrast, as discussed, Dickinson teaches that an authorized administrator enters policies by way of a configuration module in the form of a program executing on a stored program computer, but the policy modules do not themselves get attached to the e-mail in order to restrict access to the e-mail. Similarly, Motoyama et al. do not teach that that an executable module attached to the communication restricts access to and routing of the very privileged communication to which it is attached to the privileged distribution list associated with that communication.

Furthermore, claim 41 has been amended to clarify the method of creating a privileged digital communication comprises the step of configuring access rights to the digital communication and associating a privileged distribution list with the digital communication, and. enforcing the access rights based upon the privileged distribution list associated with the communication. By contrast, Dickinson teaches that an authorized administrator enters policies by way of a configuration module in the form of a program executing on a stored program computer, and these policies are applied to sent or received e-mails. However, neither Dickinson nor Motoyama teaches or suggests that a privileged distribution list is associated with the digital communication and that the access rights are enforced based upon the associated distribution list.

With regard to all other claims dependent upon independent claims 1, 18, 41, 49, 57 and 72, Applicants respectfully submit that these claims should be allowable based upon their dependencies upon base claims that are allowable, as discussed above, and that the rejections of these claims should be withdrawn.

Conclusion

Reconsideration of the present application, as amended, is requested. If, upon review, the Examiner is unable to issue an immediate Notice of Allowance, the Examiner is respectfully requested to telephone Applicant's undersigned attorney at the number set forth below in order to resolve any outstanding issues and advance the prosecution of the case.

An early and favorable action on the merits is earnestly solicited.

Respectfully submitted,
DAVIDSON, DAVIDSON & KAPPEL, LLC

By:__________________________
Morey B. Wildes
Reg. No. 36,968

Davidson, Davidson & Kappel, LLC
485 Seventh Avenue, 14th Floor
New York, NY 10018
(212) 736-1940